

UNITED STATES DISTRICT COURT
FOR THE
MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA :
 :
 vs. : No. 4:CR-04-0027
 :
 DONALD R. MILLER, Jr. : (Judge Muir)

OPINION

I. Introduction.

On January 22, 2004, an indictment was filed charging Donald R. Miller, Jr., with two counts of engaging in certain activities relating to material constituting or containing child pornography in violation of 18 U.S.C. §§ 2252A and 2256(8) (B). On November 17, 2004, the grand jury returned a superseding indictment containing four child pornography offenses in violation of 18 U.S.C. §§ 2252A and 2256(8) (B), and one count of possession of marijuana in violation of 21 U.S.C. § 844(a).

On April 11, 2005, Miller filed a document entitled "Motion to Dismiss." The filing of that motion prompted us, on April 20, 2005, to issue an order in which we continued the case to the June, 2005, Trial List, and we established a briefing schedule on Miller's "Motion to Dismiss." A brief in support of the motion was filed on May 2, 2005. The government filed its opposition brief on May 17, 2005. In its brief the government stated that a hearing was necessary to resolve the disputed facts pertaining to the motion. By order dated May 18, 2005, we continued the trial in this case to the July, 2005, Trial List, but retained the

matter on the June, 2005, Trial List for a hearing on Miller's "Motion to Dismiss." On June 6, 2005, Miller filed a reply brief in support of the motion.

On June 13, 2005, the parties filed their initial proposed findings of fact and conclusions of law. A hearing on Miller's motion to dismiss was held on June 14 and 15, 2005. At the conclusion of the hearing the parties requested, and we granted, an opportunity to file supplemental proposed findings of fact and conclusions of law by 11:30 a.m. on June 17, 2005. By order dated June 16, 2005, we confirmed that deadline. The parties timely filed their supplemental proposed findings of fact and conclusions of law.

The following are the Court's findings of fact, discussion, and conclusions of law. Findings of fact which are not disputed are noted with a "U" in parenthesis after each such finding. Findings of fact which are not disputed yet are objected to by one party are noted with a "U/O" in parenthesis after each such finding.¹

II. Findings of Fact

1. On January 13, 2004, at approximately 9:00 a.m., the Federal Bureau of Investigation executed a search warrant at the residence of Donald R. Miller, Jr., and

¹We overrule the objections to the undisputed findings of fact used herein to which there have been objections.

an arrest warrant for Miller.

2. Those actions were taken after the Federal Bureau of Investigation obtained information indicating that Miller had accessed the internet with a computer to performed certain illegal activities involving child pornography.
3. Federal Bureau of Investigation Special Agent James A. Kyle participated in the execution of those warrants.
4. Special Agent Kyle interviewed Miller and prepared a list of the evidence seized from Miller's residence.
5. Among the items seized from Miller's residence were two computer hard drives, twenty-one zip disks, and three floppy disks.
6. All of the child pornography at issue in this case is on a single zip disk seized from Miller's residence.
7. Two members of the Federal Bureau of Investigation's Computer Analysis Response Team (hereinafter "FBI CART"), James P. McDonald and Donald Justin Price, also participated in the search of Miller's residence.
8. Those member of the FBI CART took the seized computer items to their offices in Philadelphia.
9. On August 20, 2004, Miller filed a motion to compel the government to produce a mirror image copy of "one (1) computer hard drive and several 'zip' discs that were

confiscated from the defendant's home and are in the current possession of the Federal Bureau of Investigations [sic]." (Motion to compel, Document 22, p. 1)

10. Miller argued that the discovery referenced in his motion was necessary to determine if a "trojan horse" virus enabled the computer to perform certain functions without Miller's knowledge and is ultimately responsible for the presence of the illegal child pornography on Miller's computer.
11. After the motion was fully briefed, on October 6, 2004, we issued an order in which we granted Miller's motion to compel the government to produce copies of the described discovery.
12. The order of October 6, 2004, required the parties to agree on the specific terms by which the Government would provide defense counsel with image copies of the digital media in this case.
13. A stipulated protective order, pursuant to the October 6, 2004, was filed by the parties on January 11, 2005.
(U)
14. The Stipulated Protective Order filed by the parties on January 11, 2005 states that the "Government *shall* provide defense counsel, Christian D. Frey, Esquire,

with a *bit-by-bit image* of the computer hard drive and other storage media in this matter." (Emphasis added)
(U)

15. The Stipulated Protective Order, which was signed by the parties and not the court, provides in part that "[t]his stipulation shall act as a protective order regarding certain matters of discovery in this case and shall be effective without further order of the court."
16. The requirement that the government provide Miller with "a bit-by-bit image of the computer hard drive and other storage media in this matter" is referenced only in the parties' "Stipulated Protective order."
(Stipulated Protective Order, p. 1)
17. The court order of October 6, 2004, requires the government to provide Miller with "a mirror image copy of the computer hard drive and zip disks that were confiscated from Miller's home." (Order of October 6, 2004, p. 6)
18. Miller retained John R. Smith to review the computer-based discovery obtained from the government in this case.
19. Before getting involved in this case, Smith had never attempted to perform a forensic computer investigation.
20. Smith owns and for five years has operated a computer

consulting business.

21. Defendant, through a "Motion to Dismiss [Indictment]" filed April 11, 2005, has alleged, among other issues, that the Government is in violation of the Court's discovery order. (U)
22. Defendant, through a "Motion to Dismiss Indictment" filed April 11, 2005, has alleged, among other issues, that the Government has not properly preserved the evidence in this case. (U)
23. The government provided the defense with a WD400 hard drive containing copies of the digital media seized from Miller's residence.
24. Proper computer forensic procedure dictates that a target drive, in this case the WD400, be forensically wiped prior to copying evidence files to the target drive. (U)
25. There exists no chain of custody for the WD400 provided to Defense counsel. (U/O)
26. The Superseding [sic] Indictment in this case was returned on November 17, 2004. (U)
27. The WD400 presented to Defense counsel was created on November 17, 2004. (U)
28. All computer media used for purposes of prosecution under the Superseding Indictment in this case was

imaged by the FBI CART staff using standard tools, which are accepted throughout the computer forensic community. (U)

29. The Government utilized, among other programs, Encase forensic software in its examination of the computer evidence at issue. (U)
30. The members of the FBI CART who worked on the computer media seized from Miller's residence had extensive training in the use of Encase forensic software.
31. Smith had never used Encase software before being hired by Miller in connection with this case.
32. The Encase software used by Smith was purchased and provided to him by Miller.
33. In January 2005, Defense counsel for Miller was provided the same image files and computer evidence that was used in the FBI CART examination.
34. The files on the WD400 which contain the mirror images of the government's evidence are identified by the prefix "QPH."
35. Concurrent with his arrest and the seizure of the computer media, Defendant informed FBI SA James Kyle that there existed viruses on his computer that he had been having trouble with for quite some time, and that he had not been able to remove them from his computer.

(U/O)

36. A forensic examination revealed that remnants of innocuous computer viruses were found on Defendant's hard drive. (U/O)
37. The government's examination of the digital media also revealed no active computer viruses or "trojans" capable of remotely depositing child pornography on Defendant's zip disk.
38. The FBI CART has never encountered a computer virus with the capacity to perform, on its own or through an unknown remote computer user, the functions necessary to have placed the child pornography on Miller's zip disk without Miller's knowledge.
39. There exist thousands of file entries on the WD400 presented to Defense counsel in addition to the QPH image files that were supposed to be on the WD400.
(U/O)
40. Special Agent Kyle directed the FBI CART to place only two folders, each containing alleged child pornography, on the WD400 in addition to the QPH images of the evidence in this case. (U)
41. Beyond the two folders containing alleged child pornography, SA Kyle did not direct the FBI CART to place any additional information on the WD400. (U)

42. No explanation has been offered by the Government with respect to the numerous other files present on the WD400.
43. The presence of those extraneous files indicates that the WD400 may not have been forensically wiped before the FBI CART copied the QPH files onto the WD400.
44. An MDJ Hash Value is a 28 bit (16 bytes) alphanumeric value that uniquely describes the contents of a file.
(U)
45. The odds that two files with different contents have the same hash value are roughly 2 to the 128th power, or 3.2 X 10 to the 38th power. (U/O)
46. Defense counsel provided the hash values produced by John Smith's examination to the Government on March 8, 2005. (U)
47. Despite requests from Defense counsel, the Government has not provided its hash values to Defense counsel.
(U)
48. The FBI CART analyzed and compared hash values supplied by Mr. Smith. (U/O)
49. For 26 of 27 pieces of digital media turned over to the defense, the FBI CART's values matched those of Mr. Smith. (U/O)
50. The one piece of digital media for which the FBI hash

value does not match Miller's hash value is the 6.5 gigabyte hard drive.

51. Although it has attempted to do so, the FBI CART cannot reproduce Smith's hash value for that hard drive.
52. After receiving the relevant hash values from Smith, the FBI CART reviewed the hash values of the hard drive actually seized from Miller's residence (identified as QPH1_1) and the copy of that hard drive provided by the FBI CART to the defense.
53. The FBI CART review indicated that the hash value of the original piece of evidence matched the hash value of the copy of the hard drive generated by the FBI CART and provided to the defense.
54. Miller alleges that the FBI CART forensically wiped three zip disks.
55. That allegation is based on the hash values reported by Encase for the files on those three disks.
56. The FBI CART did not have any problems imaging and analyzing the zip disks other than the three(3) zip disks that Mr. Smith concludes were forensically wiped.
(U)
57. The government contends that the three zip disks were not forensically wiped and that the hash values found by Smith are the result of some other problem with the

disks, such a "read error."

58. The evidence of record does not establish that the three zip disks were forensically wiped.
59. The three unreadable zip disks contained no alleged child pornography and no data relevant to the charges.
(U/O)
60. The evidence of record does not demonstrate that any date/time stamps of the digital evidence have been altered.
61. The government provided discovery more extensive than that required by the Court's October 6, 2004, order.
62. Before the government provided copies of the digital media in this case, Special Agent Kyle gave the defense certain information, including three printed pages purporting to be a list of the contents of three floppy disks seized from Miller's residence.
63. The three printouts provided to the defense are not listings of files contained on the floppy disks examined by the FBI CART. (U/O)
64. The WD400 hard drive that the government provided to Miller in discovery in this case contains sufficient information for Miller to view bit-by-bit images of the original evidence copied onto the WD400.
65. No evidence was destroyed or altered by the Government.

66. The integrity of all digital media has been properly preserved and has not been compromised in this case.

III. Discussion.

Our threshold task is to determine the precise nature and basis of, and relief sought in, Miller's pending motion. The instant charges against Miller relate to his alleged possession of child pornography and marijuana. The primary relief discussed by Miller in his motion, proposed form of order, supporting brief, and reply brief was the dismissal of the charges against him. The only alternative form of relief referenced in the motion is "suppression of the computer media that was seized from defendant's home due to lack of preservation and subsequent compromising of the integrity of same." (Motion to Dismiss, p. 7)

None of the evidence presented at the hearing on Miller's motion to dismiss related in any manner to the marijuana offense. Consequently, nothing in the record supports the dismissal of that charge. In addition, during his opening and closing arguments at the hearing on his motion to dismiss, the only relief Miller referenced was suppression of the computer-based evidence at issue.

Those circumstances, in conjunction with Miller's failure to cite any authority supporting his position that the charges against him should be dismissed even if all of the allegations in his motion were true, compel the conclusion that Miller's motion

should actually be construed as one to exclude certain items from being introduced into evidence.

Our view of the appropriate manner to consider Miller's motion is supported not only by the specific facts of this case but also by general case law. Courts have consistently held that "[t]he sole function of a motion to dismiss is to test the sufficiency of the indictment to charge an offense. It is not a device for a summary trial of the evidence." U.S. v. Clark, 88 F. Supp. 2d 417, 419 (D.V.I. 2000); United States v. Winer, 323 F. Supp. 604, 605 (E.D. Pa.1971), citing United States v. Sampson, 71 U.S. 75, 83, 83 S. Ct. 173 (1962). Miller's pending motion does not challenge the sufficiency of the indictment in any manner. For the reasons stated above, we will construe Miller's motion as one to exclude certain items from being introduced into evidence at trial.

The second preliminary and procedural issue to address concerns assignment of the burden of proof. We raised this issue at the commencement of the hearing on Miller's motion. Each party takes the position that the other party bears the burden. If Miller's motion were based on an action taken by the government which allegedly violated his Fourth Amendment rights, the issue regarding the burden of proof would be easily resolved. In considering such a motion, "[t]ypically, the proponent of a motion to suppress bears the burden of establishing that his

Fourth Amendment rights were violated." U.S. v. Leveto, 343 F. Supp. 2d 434, 441 (W.D. Pa. 2004) (Cohill, J.) (citing United States v. Acosta, 965 F.2d 1248, 1257 n.9 (3d Cir. 1992) (citing Rakas v. Illinois, 439 U.S. 128, 130 n.1, 99 S. Ct. 421 (1978))). However, Miller's motion is not based on any such challenge.

Miller's motion to suppress implicates neither the Fourth Amendment nor any actual piece of evidence in this case. Instead, Miller's motion is grounded upon a challenge to the quality of certain discovery he received from the government. Miller argues that some of the discovery provided to him has been so badly mishandled, or compromised, that it is "forensically worthless." Despite the fact that Miller's motion to suppress rests on such an unconventional basis, we are of the view that he retains the burden of proof in connection with his motion. See *generally* United States v. Muzychka, 725 F.2d 1061, 1069-70 (3d Cir.1984) (holding that defendant's motion to suppress tape recordings on the ground that not all conversations were recorded was properly denied as "there is no evidence that [the tapes] were altered so as to give a misleading account of the recorded conversations"); see also United States v. Stewart, 104 F.3d 1377, 1383 (D.C. Cir.1997) (there is a "presumption that evidence held by government officials has been properly preserved" where a defendant challenged the chain of custody).

The burden of proof shouldered by Miller is a preponderance

of the evidence. See *United States v. Primo*, ___ F. Supp. 2d ___, 2005 WL 1076132 (W.D. Pa. 2005) (Gibson, J.) (citing *United States v. Matlock*, 415 U.S. 164, 178 n.14, 94 S. Ct. 988 (1974)).

We are now in a position to consider the substantive merits of Miller's motion. As noted above, the dispute at issue centers on the condition of certain discovery provided to Miller in response to our order of October 6, 2004. In an effort to comply with that order, the government provided Miller with a computer hard drive, identified by the parties as a WD400, on which the government had copied images of the computer evidence seized from Miller's residence and analyzed by the government. Miller argues that

[i]n reviewing the forensic reports of John Smith in conjunction with FE Price's Memo that accompanied the Brief in Opposition, it is clear that the Government indeed has not complied with this court's Order of October 6, 2004. The Government provided to defense counsel "images" of the computer evidence in this case; it did not provide the bit-by-bit copies that it was ordered to produce.

(Reply brief, p. 5)

Throughout his arguments Miller implicitly presumes that our order of October 6, 2004, imposed upon the government the obligation to provide Miller with "bit-by-bit copies" of Miller's computer media. The order includes no such reference. The government's duty to provide that information is found only in the document entitled "Stipulated Protective Order," which was signed by parties but not by the court. Despite its title, the

document at issue is a stipulation reached by the parties rather than a court order. Indeed, the first paragraph of that document states that "[t]his stipulation shall act as a protective order regarding certain matters of discovery in this case"

(Stipulated Protective Order filed on January 11, 2005, ¶1)

Furthermore, the undersigned's log for January 11, 2005, contains no entry of any order signed that day in this case and the stipulation contains no signature line for signature by the judge.

The order of October 6, 2004, required the government to produce "a mirror image copy" of the computer media. Neither party addressed the fundamental issue of whether a mirror image copy is tantamount to a "bit-by-bit copy."

Miller cites the testimony and report of John R. Smith in support of his conclusion that the discovery at issue has been tainted or altered to the point that the original evidence should be suppressed. At the hearing on Miller's motion, Miller attempted to qualify Smith as an expert witness in the fields of computer virus detection and analysis and forensic computer examinations. The government objected to Smith's testimony, contending that he is not an expert in those fields. When the government's objection arose we orally withheld ruling on it and allowed Smith to testify as though he had been qualified as an expert.

Our disposition of Miller's motion is in no way affected by our decision with respect to whether Smith is or is not an expert in the fields proffered by Miller. Strictly for the purposes of this order, we will accept his testimony as if he had been qualified as an expert in computer information storage. Our ruling regarding Smith's testimony for the purposes of this order is based on the fact that Smith's experience with computer software and the storage of information on a computer enabled him to present and explain relatively complicated computer concepts to the court. The government may challenge Smith's designation as any type of expert in the trial of this case.

The government's case at the hearing on Miller's motion consisted primarily of the testimony provided by Special Agent James Kyle, and FBI CART members Justin Price, James McDonald, and James Fottrell. Those four witnesses were offered and accepted, without objection, as experts in their respective fields. Special Agent Kyle investigates the sexual exploitation of children through the use of computers and the internet, and the other three agents work on the FBI CART in the field of computer forensics. Agent Fottrell's work specifically deals with computer viruses, including trojan viruses.

The essence of Smith's testimony is that the existence on the WD400 of information beyond the QPH images shows that the government has mishandled the underlying evidence and violated

the order of October 6, 2004, as well as the parties' "Stipulated Protective Order" filed on January 11, 2005. Of particular note are the following circumstances emphasized by Miller: 1) two versions of images of the six megabyte hard drive exist on the WD400; 2) three of the zip disks appear to have been forensically wiped, or for some other reason appear to contain absolutely no information; 3) some of the files presented on the WD400 have a "last written" date of January 14, 2004, which is after they had been seized from Miller; 4) the table of contents provided by the government does not match the actual contents of three floppy disks; and 5) thousands of unexplained file entries on the WD400.

Miller employs those facts as a springboard to question the government's handling of the original evidence in this case. However, Miller has failed to make any connection between the information presented on the WD400 and the actual evidence in this case. Miller's arguments are strictly limited to the condition of the discovery provided to him. Consequently, it appears as though Miller's pending motion should actually have been framed as one to compel the government to produce the discovery as required by the order of October 6, 2004, and the parties' stipulated protective order. However, the motion has not been presented as such and we will not consider whether Miller is entitled to that type of relief.

To the extent that Miller's motion could be construed as

being based on an alleged violation by the government of a court order, he has failed to meet his burden of establishing a violation of either the court order of October 6, 2004, or the parties' "Stipulated Protective Order" filed on January 11, 2005. In our view none of the circumstances referenced in Smith's testimony violates either the court order of October 6, 2004, or the parties' "Stipulated Protective Order" filed on January 11, 2005. While Smith's testimony raises potential questions about the manner in which the WD400 had been prepared, none of those grounds justifies the suppression of any evidence.

Despite Smith's contentions concerning the condition of the discovery provided to the defense, the evidence introduced at the hearing on Miller's motion indicates that the WD400 hard drive provided to Miller in discovery in this case contains sufficient information for Miller to view accurate images of the original evidence copied onto the WD400.

It is also significant that the only possibility regarding any inconsistent information on the WD400 relates to the two images of the 6.5 megabyte hard drive on the WD400. As noted above, the hash values of the computer media images match for 26 of the 27 relevant items. The sole discrepancy relates to the 6.5 megabyte hard drive.

Although the government's case against Miller is not based on any information on that hard drive, the two following

explanations were offered by the government with respect to those images: 1) the government initially copied an Encase version of the image onto the WD400 and then copied a second image after realizing that Miller may not have had access to software capable of reading an Encase file; and 2) the hash values of the two images would be different as a result of compressing files and using different software to transfer the image. Although Miller disputed the first explanation, he failed to address the second. We further note that although the hash values apparently differ between the two images of the six megabyte hard drive, there is no evidence that the actual images contained within the two image files differ.

The one argument presented by Miller which relates to the potential loss of some information concerns the three zip disks which are blank. The parties offered conflicting explanations for such a condition; Miller contends that the government forensically wiped them, and the government asserts that the disks have suffered some type of damage which results in a "read error" when attempting to access the information on the disk. Miller has not met his burden of establishing that his is the only or most likely explanation. Moreover, at this point those three zip disks appear to be of only marginal importance because no inculpatory or exculpatory information has been attributed to them by either party.

The evidence presented at the hearing leads us to conclude that while the information on the WD400 may not be a bit-by-bit image of the government's evidence, there is sufficient information on the WD400 for the defense, with minimal effort, to obtain such images. Although the information provided by the government may not have been in the format anticipated by Miller and Smith, we are of the view that the government has fulfilled both the letter and spirit of the order of October 6, 2004, and the parties' "Stipulated Protective Order" filed on January 11, 2005.

Miller has not met his burden of demonstrating a reason to suppress any of the computer evidence at issue in this case. We will deny his motion to dismiss the indictment or in the alternative suppress any evidence.

IV. Conclusions of law.

1. Miller's arguments do not relate to the sufficiency of the indictment.
2. Miller's arguments are not based on any actual evidence seized from Miller's residence.
3. Miller's arguments are not based on any alleged violation of the Fourth Amendment.
4. Strictly for the purposes of this order, John R. Smith qualifies as an expert witness under Federal Rule of Evidence 702 in the field of computer information

storage.

5. Government witness James Kyle qualifies as an expert witness under Federal Rule of Evidence 702 in the field of the sexual exploitation of children through the use of computers and the internet.
6. Government witness Justin Price qualifies as an expert witness under Federal Rule of Evidence 702 in the field of forensic computer examinations.
7. Government witness James P. McDonald qualifies as an expert witness under Federal Rule of Evidence 702 in the field of forensic computer examinations.
8. Government witness James Fottrell qualifies as an expert witness under Federal Rule of Evidence 702 in the field of forensic computer examinations, specifically viruses including "trojan" viruses.
9. In order to prevail on his motion Miller is required to demonstrate his entitlement to relief by a preponderance of the evidence.
10. The integrity of all digital media has been properly preserved and has not been compromised in this case.
11. The government did not violate either the court order of October 6, 2004, or the stipulated protective order filed by the parties on January 11, 2005.
12. Miller has not presented any reason to dismiss the

indictment or suppress any evidence in this case.
An appropriate order will be entered.

s/Malcolm Muir
MUIR, U.S. District Judge

DATED: June 22, 2005

MM:ga

UNITED STATES DISTRICT COURT
FOR THE
MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA :
 :
 vs. : No. 4:CR-04-0027
 :
 DONALD R. MILLER, Jr. : (Judge Muir)

ORDER

June 22, 2005

1. Miller's "Motion to Dismiss" (Document 61) is denied.
2. The jury will be drawn beginning at 10:00 a.m. on July 6, 2005, and because there are no other jury cases remaining on our July, 2005, trial list, trial in this case will commence immediately thereafter.

s/Malcolm Muir
MUIR, U.S. District Judge

MM:ga